

(19) 日本国特許庁(JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 10-63722

(43) 公開日 平成10年(1998)3月6日

(51) Int. Cl. °	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 17/60			G 0 6 F 15/21 3 4 0 D	
G 0 7 D 9/00	4 3 6		G 0 7 D 9/00 4 3 6 Z	
G 0 7 F 7/08			G 0 7 F 7/08 Z	

審査請求 未請求 請求項の数 7

O L

(全 10 頁)

(21) 出願番号 特願平 8-214747

(22) 出願日 平成8年(1996)8月14日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 廣川 勝久

東京都港区芝浦一丁目1番1号 株式会社東芝
芝本社事務所内

(72) 発明者 茂田井 省三

東京都港区芝浦一丁目1番1号 株式会社東芝
芝本社事務所内

(72) 発明者 田中 陽子

東京都港区芝浦一丁目1番1号 株式会社東芝
芝本社事務所内

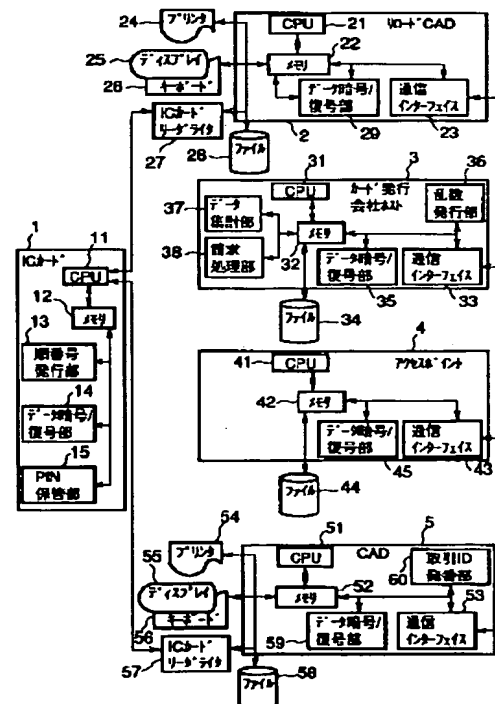
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 カード取引システム及びカード取引方法

(57) 【要約】

【課題】 信用照会にかかるコストを最小限にして、しかもセキュリティを向上させる。

【解決手段】 リロードCAD2がICカードリーダライタ27に挿入されるICカード1から与信の補填指示を受け、カード発行会社ホスト3と通信し、カード発行会社ホスト3の承認(信用照会)後、ICカード1へ与信を補填し、店舗に備えられたCAD5が取引の際、カード発行会社ホスト3と通信による信用照会を行わずにICカード1からの与信を受け付け、所定の時間に取引データをアクセスポイント4へ送信し、アクセスポイント4が多数存在するCAD5のデータを受け付け、そのデータを所定のカード発行会社ホスト3に振り分け、カード発行会社ホスト3が取引データを受け付けて請求処理を行う。



【特許請求の範囲】

【請求項 1】 カード発行会社から発行されたカードで取引を行うカード取引方法であって、

上記カードを用いた所定金額の使用権利が上記カード発行会社に信用照会して承認された際、承認された所定金額の使用権利を上記カードに補填し、補填された上記カードが所定金額分を上記カード発行会社への信用照会なしで取引できるようにしたことを特徴とするカード取引方法。

【請求項 2】 カード発行会社のホストコンピュータとカード発行会社から発行されたカードとこのカードに所定金額の使用権利を補填する補填装置とから構成されるカード取引システムにおいて、

上記カード発行会社のホストコンピュータが、上記カードの信用照会を行って上記カードに対する所定金額の信用照会なしで使用する権利を承認する承認手段を有し、

上記補填装置が、上記承認手段で上記カードに対する所定金額の信用照会なしで使用する権利が承認された際、上記カードに所定金額の使用権利を補填する補填手段を有し、

上記カードが、上記補填手段により補填される所定金額の信用照会なしで使用する権利の情報を記憶する記憶手段と、を具備したことを特徴とするカード取引システム。

【請求項 3】 カード発行会社から発行された第 1 のカードを用いて取引を行うカード取引方法であって、上記第 1 のカードの信用照会を行って所定金額の使用権利が上記カード発行会社に承認された際、承認された所定金額の使用権利を上記第 1 のカードに予め登録されている識別子に対応する第 2 のカードに補填し、この第 2 のカードに補填された所定金額分が上記カード発行会社への信用照会なしで取引できるようにしたことを特徴とするカード取引方法。

【請求項 4】 カード発行会社から発行される第 1 のカードと、カード発行会社のホストコンピュータとカード補填装置とが接続されて構成されるカード取引システムにおいて、

上記カード発行会社のホストコンピュータが、上記第 1 のカードの信用照会を行って上記第 1 のカードに対する所定金額の信用照会なしで使用する権利を承認する承認手段を有し、

上記カード補填装置が、上記承認手段で上記第 1 のカードに対する所定金額の信用照会なしで使用する権利が承認された際、上記第 1 のカードに予め登録されている識別子に対応する第 2 のカードに所定金額の使用権利を補填する補填手段と、を具備したことを特徴とするカード取引システム。

【請求項 5】 カード発行会社から発行されるカードと、カード発行会社のホストコンピュータとカード補填

装置とが接続されて構成されるカード取引システムにおいて、

上記カードが、上記ホストコンピュータに信用照会を行って所定金額の信用照会なしで使用する権利を承認させる指示を行う承認指示手段と、

この承認指示手段により上記ホストコンピュータが承認した際、上記カード補填装置から補填される所定金額の信用照会なしで使用する権利の情報を記憶する記憶手段と、

この記憶手段に記憶された所定金額分を上記カード発行会社のホストコンピュータに信用照会なしで取引する所定金額の残金制御手段と、を具備したことを特徴とするカード取引システム。

【請求項 6】 カード発行会社から発行されるカードと、カード発行会社のホストコンピュータとカード補填装置とが接続されて構成されるカード取引システムにおいて、

上記カード発行会社のホストコンピュータが、乱数を発行する乱数発行手段と、この乱数発行手段で発行された乱数の情報を上記カードに通知する第 1 の通知手段と、

上記カードが、上記第 1 の通知手段から通知される乱数情報を受信する第 1 の受信手段と、

この第 1 の受信手段で受信された乱数に基づいて認証子を算出する第 1 の算出手段と、

この第 1 の算出手段で算出された認証子を上記カード発行会社のホストコンピュータに通知する第 2 の通知手段と、

さらに上記カード発行会社のホストコンピュータが、上記第 2 の通知手段から通知される認証子を受信する第 2 の受信手段と、

上記乱数発行手段で発行された乱数に基づいて認証子を算出する第 2 の算出手段と、

この第 2 の算出手段で算出された認証子と上記第 2 の受信手段で受信された認証子とを比較する比較手段と、

この比較手段の比較結果が一致した場合に上記カードの正当を承認する承認手段と、

を具備したことを特徴とするカード取引システム。

【請求項 7】 カード発行会社から発行されたカードで想定できない乱数を上記カード発行会社のホストコンピュータが発行して上記カードに通知し、上記カードがその乱数に基づいて認証子を算出して上記ホストコンピュータへ通知し、上記ホストコンピュータも上記乱数に基づいて認証子を算出して上記カードから通知された認証子と比較し、比較結果によって上記カードが正当なカードであることを証明することを特徴とするカードの証明方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、所定金額の使用権利を補填するカードに与信を予め一括して承認し、取引の都度の信用照会を省略するカード取引システム及びカード取引方法に関する。

【0002】

【従来の技術】従来、クレジットカード等を使用して取引を行う場合、取引の可否を確認するために取引先はカード発行会社に、その都度信用照会を行う必要があった。信用照会には費用が発生するため、信用照会を行わなければならない取引金額を規定し、それ以下の場合は信用照会無しで取引を行って費用を節約する方法も取られているが、不正利用防止の目的から、規定された取引金額は1円（ゼロフロアリミットと呼ばれている）以上からであることが多く、現状ではほとんどすべての取引にこの方式で信用照会が行われている。

【0003】しかしながら、信用照会は、カード発行会社ホストへの通信費、信用照会料等のコストがかかり、小口の取引ではそのコストによって利益が出ないこともある。一方、信用照会を行わなければ、カードの不正使用を確認できず、被害が無制限に広がるおそれがある。

【0004】

【発明が解決しようとする課題】上記したように、クレジットカード等を使用して取引を行う場合、取引の可否を確認するために取引先はカード発行会社に、その都度信用照会を行う必要があり、信用照会は、カード発行会社ホストへの通信費、信用照会料等のコストがかかり、小口の取引ではそのコストによって利益が出ないという問題と、信用照会を行わなければ、カードの不正使用を確認できず、被害が無制限に広がるおそれがあるというセキュリティに問題があった。

【0005】そこで、この発明は、信用照会にかかるコストを最小限にして、しかもセキュリティを向上させることのできるカード取引システム及びカード取引方法を提供することを目的とする。

【0006】

【課題を解決するための手段】この発明のカード取引方法は、カード発行会社から発行されたカードで取引を行うカード取引方法であって、上記カードを用いた所定金額の使用権利が上記カード発行会社に信用照会して承認された際、承認された所定金額の使用権利を上記カードに補填し、補填された上記カードが所定金額分を上記カード発行会社への信用照会なしで取引できるようにしたことを特徴とする。

【0007】この発明のカード取引システムは、カード発行会社のホストコンピュータとカード発行会社から発行されたカードとこのカードに所定金額の使用権利を補填する補填装置とから構成されるカード取引システムにおいて、上記カード発行会社のホストコンピュータが、上記カードの信用照会を行って上記カードに対する所定

金額の信用照会なしで使用する権利を承認する承認手段を有し、上記補填装置が、上記承認手段で上記カードに対する所定金額の信用照会なしで使用する権利が承認された際、上記カードに所定金額の使用権利を補填する補填手段を有し、上記カードが、上記補填手段により補填される所定金額の信用照会なしで使用する権利の情報を記憶する記憶手段とから構成されている。

【0008】この発明のカード取引方法は、カード発行会社から発行された第1のカードを用いて取引を行うカード取引方法であって、上記第1のカードの信用照会を行って所定金額の使用権利が上記カード発行会社に承認された際、承認された所定金額の使用権利を上記第1のカードに予め登録されている識別子に対応する第2のカードに補填し、この第2のカードに補填された所定金額分が上記カード発行会社への信用照会なしで取引できるようにしたことを特徴とする。

【0009】この発明のカード取引システムは、カード発行会社から発行される第1のカードと、カード発行会社のホストコンピュータとカード補填装置とが接続されて構成されるカード取引システムにおいて、上記カード発行会社のホストコンピュータが、上記第1のカードの信用照会を行って上記第1のカードに対する所定金額の信用照会なしで使用する権利を承認する承認手段を有し、上記カード補填装置が、上記承認手段で上記第1のカードに対する所定金額の信用照会なしで使用する権利が承認された際、上記第1のカードに予め登録されている識別子に対応する第2のカードに所定金額の使用権利を補填する補填手段とから構成されている。

【0010】この発明のカード取引システムは、カード発行会社から発行されるカードと、カード発行会社のホストコンピュータとカード補填装置とが接続されて構成されるカード取引システムにおいて、上記カードが、上記ホストコンピュータに信用照会を行って所定金額の信用照会なしで使用する権利を承認させる指示を行う承認指示手段と、この承認指示手段により上記ホストコンピュータが承認した際、上記カード補填装置から補填される所定金額の信用照会なしで使用する権利の情報を記憶する記憶手段と、この記憶手段に記憶された所定金額分を上記カード発行会社のホストコンピュータに信用照会なしで取引する所定金額の残金制御手段とから構成されている。

【0011】この発明のカード取引システムは、カード発行会社から発行されるカードと、カード発行会社のホストコンピュータとカード補填装置とが接続されて構成されるカード取引システムにおいて、上記カード発行会社のホストコンピュータが、乱数を発行する乱数発行手段と、この乱数発行手段で発行された乱数の情報を上記カードに通知する第1の通知手段と、上記カードが、上記第1の通知手段から通知される乱数情報を受信する第1の受信手段と、この第1の受信手段で受信された乱数

に基づいて認証子を算出する第1の算出手段と、この第1の算出手段で算出された認証子を上記カード発行会社のホストコンピュータに通知する第2の通知手段と、さらに上記カード発行会社のホストコンピュータが、上記第2の通知手段から通知される認証子を受信する第2の受信手段と、上記乱数発行手段で発行された乱数に基づいて認証子を算出する第2の算出手段と、この第2の算出手段で算出された認証子と上記第2の受信手段で受信された認証子とを比較する比較手段と、この比較手段の比較結果が一致した場合に上記カードの正当を承認する承認手段とから構成されている。

【0012】この発明のカードの証明方法は、カード発行会社から発行されたカードで想定できない乱数を上記カード発行会社のホストコンピュータが発行して上記カードに通知し、上記カードがその乱数に基づいて認証子を算出して上記ホストコンピュータへ通知し、上記ホストコンピュータも上記乱数に基づいて認証子を算出して上記カードから通知された認証子と比較し、比較結果によって上記カードが正当なカードであることを証明することを特徴とする。

【0013】

【発明の実施の形態】以下、この発明の一実施の形態について図面を参照して説明する。図1は、この発明に係るカード取引システムの概略構成を示すものである。すなわち、カード取引システムは、カード発行会社の発行したICカード1、与信の補填を行うためのリロードCAD (Card Acceptance Device) 2、カード発行会社のホスト3、アクセスポイント4、取引を行うために店舗に備えられたCAD (Card Acceptance Device) 5とから構成されている。

【0014】ICカード1には、図示していないが与信の補填を指示できるクレジット機能を備えた与信カード1a、与信の補填を行ってその与信で取引を行える補填カード1bとが存在し、与信カードと補填カードの機能が一体となったICカード1cも存在する。

【0015】これらのICカード1、1a、1b、1cは、ともに同じ構成であるので、図示しているICカード1で構成を説明する。すなわち、ICカード1は、CPU11、メモリ12、順番号発行部13、データ暗号／復号部14、PIN保管部15で構成されている。

【0016】CPU11は、後述するICカードリーダライタ27または57とのデータとコマンドの授受、PIN保管部15に存在するPIN (Personal Identification Number: 個人識別番号) チェックを行う。記憶手段としてのメモリ12には、処理に必要な各データが記録されている。順番号発行部13は、補填された与信を使用して取引を行う際に、支払われる与信に対してユニークな順番号を発行する。発行された順番号は与信とともに取引相手に支払われ、与信の重複チェックを行うのに使用される。

【0017】データ暗号／復号部14は、リロードCAD2またはCAD5へ送るデータの暗号、リロードCAD2またはCAD5からの暗号化されたデータの復号を行うとともに、カード発行会社ホスト3から通知された乱数をもとに認証子を算出する。

【0018】リロードCAD2は、与信の補填指示を受け、カード発行会社ホスト3と通信し、カード発行会社ホスト3の承認後所定のICカード1へ与信を補填するCAD (Card Acceptance Device) であり、CPU21、メモリ22、通信インターフェース23、プリンタ24、ディスプレイ25、キーボード26、ICカードリーダライタ27、ファイル28、データ暗号／復号部29で構成されている。

【0019】CPU21は、各装置の制御を行い、ICカード1とのデータの授受、データチェック、ICカード1へのデータ書込等の指示を行う。メモリ22には、各種データが記録される。通信インターフェース23はカード発行会社ホスト3とのデータ授受を行い、そのデータはメモリ22に展開される。

【0020】プリンタ24は、補填が完了した際の証書を発行する。ディスプレイ25は、与信の補填処理に必要なメッセージまたはデータの表示を行う。キーボード26は与信の補填を指示する際のPIN、補填先の入力を受け付け、そのデータをメモリ22に渡す。ICカードリーダライタ27は、ICカード1のデータの読取りまたは書込みを行う。

【0021】ファイル28には、補填処理に必要なソフトウェア、データが格納されている。データ暗号／復号部29は、ICカード1、またはカード発行会社ホスト3へ送るデータの暗号、ICカード1またはカード発行会社ホスト3からの暗号化されたデータの一部の復号を行う。

【0022】カード発行会社ホスト3は、発行したICカード1の所有者 (カードホルダ) の与信状態をもとに取引の承認を行い、取引データを受け付けて各ICカード1の所有者 (カードホルダ) に後日請求し、取引した金額を各店舗に支払う。カード発行会社ホスト3は、CPU31、メモリ32、通信インターフェース33、ファイル34、データ暗号／復号部35、乱数発行部36、データ集計部37、請求処理部38で構成されている。

【0023】CPU31は各装置の制御を行う。メモリ32には各種データが記録される。通信インターフェース33は、リロードCAD2、アクセスポイント4とのデータ授受を行い、そのデータはメモリ32に展開される。ファイル34には、与信の補填、取引データの集計、請求に必要なソフトウェア及び各データが格納されている。

【0024】データ暗号／復号部35は、リロードCAD2またはアクセスポイント4へ送るデータの暗号、リ

ロードCAD2またはアクセスポイント4からの暗号化されたデータの復号を行うとともに、乱数発行部36が発行した乱数をもとに認証子を算出する。乱数発行部36は、ICカード1が与信を補填しても良いカードかどうかを証明するために乱数を発行する。この乱数はICカード1に通知され、この乱数をもとにICカード1は認証子を算出し、結果をカード発行会社ホスト3に通知する。

【0025】データ集計部37は、アクセスポイント4から送られた取引データをICカード1毎に集計する。集計したデータは取引された与信の値が、予め補填した与信を超えていないかのチェックに用いられる。請求処理部38は、取引データをもとにICカード1の所有者（カードホルダ）への請求を行う。

【0026】アクセスポイント4は、多数存在するCAD5のデータを受け付け、そのデータを所定のカード発行会社ホスト3に振り分ける。アクセスポイント4は、CPU41、メモリ42、通信インターフェース43、ファイル44、データ暗号/復号部45で構成されている。CPU41は各装置の制御を行う。メモリ42には各種データが記録される。通信インターフェース43はカード発行会社ホスト3、CAD5とのデータ授受を行い、そのデータはメモリ42に展開される。ファイル44には、データの振り分けに必要なソフトウェア、データが格納されている。データ暗号/復号部45は、CAD5からカード発行会社ホスト3へ、またはカード発行会社ホスト3からCAD5へ送る暗号化されたデータの一部復号を行う。

【0027】CAD5は、取引の際にICカード1からの与信を受け、所定の時間に取引データをアクセスポイント4へ送信するCAD（Card Acceptance Device）であり、CPU51、メモリ52、通信インターフェース53、プリンタ54、ディスプレイ55、キーボード56、ICカードリーダライタ57、ファイル58、データ暗号/復号部59、取引ID発番部60で構成されている。

【0028】CPU51は、各装置の制御を行い、ICカード1とのデータの授受、データチェック、ICカード1へのデータ書込等の指示を行う。メモリ52には各種データが記録される。通信インターフェース53はカード発行会社ホスト3とのデータ授受を行い、そのデータはメモリ52に展開される。プリンタ54は、取引が完了した際の証書を発行する。

【0029】ディスプレイ55は、取引処理に必要なメッセージまたはデータの表示を行う。キーボード56は、与信が不足していた場合の与信値入力を受け付け、そのデータをメモリ52に渡す。ICカードリーダライタ57は、ICカード1のデータの読取りまたは書込みを行う。ファイル58には、取引処理に必要なソフトウェア、データが格納されている。

【0030】データ暗号/復号部59は、ICカード1、またはカード発行会社ホスト3へ送るデータの暗号、ICカード1またはカード発行会社ホスト3からの暗号化されたデータの一部の復号を行う。取引ID発番部60は、取引データを作成する際に取引IDを発番する。取引IDは、取引データに対してユニークにつけられ、取引データの重複チェックに使用される。

【0031】図2は、各処理におけるICカード1（与信カード1aと補填カード1b）、リロードCAD2、CAD5、カード発行会社ホスト3、アクセスポイント4間のデータの流れの概要を示している。

【0032】本発明での処理は、以下のステップに大別される。各ステップの詳細は、後述する図3以降のタイミングチャートに記述される。

図2の（a）に示すステップ1：補填カード1bへの与信の補填。

【0033】ここでは、与信を付与できる与信カード（ICカード）1aを使用して与信の補填を指示し、補填カード（所定のカード）1bに承認された与信を補填する。まず、与信カード1aをリロードCAD2に挿入して与信の補填を行う。補填指示を受けたリロードCAD2は、与信カード1aのデータと補填する金額をカード発行会社ホスト3へ送信する。データを受け付けたカード発行会社ホスト3は指定された金額の承認を行っても良いか確認し、良い場合は与信をリロードCAD2へ送信する。リロードCAD2は、与信を所定の補填カード1bへ送信して補填する。

【0034】図2の（b）に示すステップ2：補填カード1bによる店舗での取引。

ここでは、与信の補填された補填カード1bを使用して店舗（実際の店舗または仮想の店舗）に備えられたCAD5との取引を行う。取引を行うと補填カード1b内の与信が取引額分減算され、取引データがCAD5にて作成され、一時保管（タンキング）される。

【0035】図2の（c）に示すステップ3：カード発行会社へのデータ送信。

ここでは、複数のCAD5において、それぞれのCAD5に一時保管された取引データを所定の時間にアクセスポイント4へ一括して送信（データキャプチャー）し、アクセスポイント4は各取引データを所定のカード発行会社ホスト3へ振り分け、取引データを受け付けたカード発行会社ホスト3が請求処理を行う。

【0036】次に、このような構成においてICカードの処理動作を図3から図6のタイミングチャートを参照して説明する。図3から図6は、各ステップでのリロードCAD2またはCAD5、ICカード1、アクセスポイント4、カード発行会社ホスト3の処理を示すタイミングチャートである。

【0037】図3と図4は、ステップ1：補填カード（ICカード）1bへの与信の補填処理のタイミングチ

ャートである。ここでは、ICカード（与信カード1 a、補填カード1 b）、リロードCAD2、カード発行会社ホスト3間でデータをやりとりし、処理を行う。なお、データは必要に応じて各装置が持つデータ暗号／復号部14、29、35、45、59で暗号化されて送信され、受信した装置は自分の持つデータ暗号／復号部14、29、35、45、59で必要に応じて復号しても良い。

【0038】補填カード（ICカード）1 bがリロードCAD2のICカードリーダライタ27に挿入されると、ステップ1-1で補填カード1 bからリロードCAD2へ補填カード1 bの与信残高が通知される。ステップ1-2では、リロードCAD2が補填カード1 bの与信残高を取得して必要な補填金額を算出する（または補填カード1 bが必要な補填金額を算出してリロードCAD2に通知してもよい）。なお、補填の方法が、補填カード1 b内にある与信残高にかかわらず一定金額を上書きする方式の場合、ステップ1-1と1-2は不要である。

【0039】与信カード（ICカード）1 aがリロードCAD2のICカードリーダライタ27に挿入されると、ステップ1-3で与信カード1 aからリロードCAD2へ与信カード1 aのデータが通知される。データの通知を受けたリロードCAD2は、ステップ1-4で与信カード1 aから与信カード1 aのID（アカウントID）、及びこの与信カード1 aから与信を補填することのできる補填カード1 bのID（1から複数）を受け付ける（オフラインの与信取引：クレジットを許容したカードである場合、オフラインで取引した金額もこの時通知する）。

【0040】この時、取引データの中に補填カード1 bのIDが1または複数存在するが、複数の場合、ステップ1-5のようにリロードCAD2は補填先の候補をディスプレイ25へ表示し、ステップ1-6でキーボード26から入力された補填先を受け付ける（補填先が複数存在する場合に行う）。

【0041】ステップ1-7でリロードCAD2のキーボード26から入力されるPIN（Personal Identification Number：個人識別番号）が受け付けられ、ステップ1-8で与信カード1 aへ通知する。通知を受けた与信カード1 aは、ステップ1-9で通知されたPINと与信カード1 a内のPIN保管部15に保管されているPINとを比較し、ステップ1-10で判定をリロードCAD2へ通知する。

【0042】判定を受けたリロードCAD2は、ステップ1-11で判定をチェックし、判定がNGであればステップ1-12のようにNGメッセージをディスプレイ25に表示して、処理を中断する。判定がOKであれば、ステップ1-13のように与信カード1 aのアカウントID、補填カード1 bのID、与信金額をカード発

行会社ホスト3へ通知する。

【0043】通知を受けたカード発行会社ホスト3は、ステップ1-14でアカウントIDが存在するかをファイル28を参照してチェックする。その後、ステップ1-15でファイル28の与えても良い与信の利用限度額から利用金額をひいた金額（利用可能金額）を算出し、そのカードが通知を受けた分だけの与信金額よりも大きいかを確認し、承認しても良いかをチェックする。さらにステップ1-16で補填先IDが正しいかどうかをファイル28を参照してチェックする。これらチェックが完了したら、ステップ1-17で判定結果をリロードCAD2へ通知し、これを受けたリロードCAD2はステップ1-18で判定結果をディスプレイ25に表示する。

【0044】ステップ1-17の次にカード発行会社ホスト3は、ステップ1-19で与信金額分の与信をホールド、つまりファイル34内の利用金額を今回承認する金額分加算し、ステップ1-20で与信ホールド通知をリロードCAD2へ通知する。通知を受けたリロードCAD2は、ステップ1-21で与信補填準備完了の表示をディスプレイ25に表示する。

【0045】与信補填準備完了後、補填カード1 bがリロードCAD2のICカードリーダライタ27へ挿入されると、ステップ1-22で補填カードデータが補填カード1 bからリロードCAD2へ通知される。なお、1枚のICカード1が、補填カードと与信カードの機能を備えている場合、このステップは不要であり、自動的に処理はステップ1-21からステップ1-23へ移る。

【0046】ステップ1-23では、補填カード1 bを受け付けたことをカード発行会社ホスト3へ通知する。通知を受けたカード発行会社ホスト3は、ステップ1-24で乱数を発行し、ステップ1-25でこれを補填カード1 bへ通知する。通知を受けた補填カード1 bは、ステップ1-26で補填カードID、データ暗号／復号部14にある暗号・復号鍵、通知された乱数をもとに暗号・復号部14で認証子を算出する。

【0047】算出後、ステップ1-27で認証子をカード発行会社ホスト3へ通知する。通知を受けたカード発行会社ホスト3も、ステップ1-28で補填カード1 bで行ったのと同じ方法で認証子を算出し、ステップ1-29で補填カード1 bから通知された認証子とカード発行会社ホスト3が算出した認証子との比較を行い、両者が同一かを確認する。

【0048】確認後、ステップ1-30で判定をリロードCAD2へ通知する。通知を受けたリロードCAD2はステップ1-31で判定を判断し、判定がNGの場合はステップ1-32のようにNGメッセージをディスプレイ25へ表示し、判定がOKの場合はステップ1-33のように与信の補填、つまり補填カード1 bのメモリ12内の与信残高の書換を行う。その後、リロードCA

D2は、与信を補填したことを示す証書をプリンタ24から出力する。

【0049】図5は、ステップ2：補填カードによる店舗での取引処理のタイミングチャートである。ここでは、ICカード（補填カード1b）、CAD5間でデータをやりとりし、処理を行う。支払いのためにカードホルダ（所有者）または店員が補填カード1bをCAD5のICカードリーダライタ57に挿入すると、ステップ2-1で補填カード1bが補填カードデータを通知し、ステップ2-2でCAD5が補填カード1b内の与信残高を取得する。

【0050】ステップ2-3でCAD5は残高のチェックを行い、支払うべき金額分の与信が補填カード1bにあるか確認する。与信がない、または不足している場合は、ステップ2-4で現金を要求する旨のメッセージをディスプレイ55へ表示し、不足している場合はステップ2-5で与信で支払う金額の入力の要求も行い、ステップ2-6で与信で支払う金額をキーボード56から受け付ける。

【0051】与信が十分にある場合、または不足していて一部を与信で支払う場合、ステップ2-7においてCAD5は補填カード1bから減算すべき与信の金額を算出して補填カード1bへ通知する。通知を受けた補填カード1bはステップ2-8でメモリ12内の与信残高を減算し、順番号発行部13にて順番号を発行し、ステップ2-9で順番号とし減算した与信金額をCAD5へ通知する。

【0052】通知を受けたCAD5は、ステップ2-10において取引ID発番部60で取引IDを発番して、ステップ2-11で取引データを作成、一時保管する。その後、CAD5は、取引完了のメッセージをディスプレイ55へ表示し、レシートをプリンタ54から発行する。

【0053】図6は、ステップ3：カード発行会社ホスト3へのデータ送信処理のタイミングチャートである。ここではCAD5、アクセスポイント4、カード発行会社ホスト3間でデータをやりとりし、処理を行う。予め定めた時間にCAD5は、ステップ3-1で一時保管していた取引データをアクセスポイント4へ送信する。データを受けたアクセスポイント4は、ステップ3-2でデータ内の取引IDがファイル44に保管してある受信済みデータの取引IDと重複していないかを確認後、それぞれのカード発行会社ホスト3へ転送する。

【0054】カード発行会社ホスト3は、ステップ3-4で取引データ内のカードIDと与信順番号がファイル34にある受信済み取引データと重複していないか、ステップ3-5で取引IDがファイル34にある受信済み取引データと重複していないかを確認する。さらに一定の時期にステップ3-6で取引データを与信カードID（補填カードIDから判断可能）毎に集計し、ステップ

3-7で合計取引金額が与信として補填した金額を超えていないかを確認後、請求処理部38へ請求すべき金額を通知する。通知を受けた請求処理部38は、ステップ3-8で与信カード1aの所有者（カードホルダ）に対して請求を行う。

【0055】図7は、上記処理に必要な、ICカード（与信カード1a）、ICカード（補填カード1b）、リロードCAD2、CAD5、アクセスポイント4、及びカード発行会社ホスト3における保持データの例である。

【0056】ICカード（与信カード1a）は、アカウントID、補填カードID（1～n）、与信可能限度額、カードの有効期限、与信付与方式、PIN、暗号／復号鍵等である。なお、補填カードID（1～n）は手入力の場合もあり、与信付与方式も手入力の場合もある。また、与信付与方式は、金額追加方式または金額上書き方式のいずれかである。

【0057】ICカード（補填カード1b）は、補填カードID、与信残高、与信受け取り限度額、与信の有効期限、カードの有効期限、発番済み与信順番号、暗号／復号鍵等である。

【0058】リロードCAD2は、端末ID、暗号／復号鍵等である。CAD5は、端末ID、発番済み取引ID、暗号／復号鍵等である。アクセスポイント4は、受付済み取引ID、暗号／復号鍵等である。

【0059】カード発行会社ホスト3は、与信カードに対する補填カードID（1～複数）、与信カード保持者の与信利用限度額、補填済み与信高、有効期限、使用した補填与信高、暗号／復号鍵、乱数発行用パラメータ等である。

【0060】以上説明したように上記発明の実施の形態によれば、信用照会を一括して前もって行うことにより、取引時の信用照会が省略でき、従って信用照会に伴うコスト、時間を省略することができる。

【0061】また、従来のクレジット処理では、取引を行う都度の信用照会を行っており、このため取引には信用照会のコストと時間がかかっていたが、一括して承認しておくことにより、取引時のコストと時間を省略することができる。

【0062】また、与信をカードに補填する際に必要なデータをすべてカードに保管しておき、そこから自動入力することにより与信補填時の利便性が増す。さらに、1枚のカードで承認指示と承認データの登録を連動させることにより、承認データの登録時の利便性とセキュリティが向上する。

【0063】また、承認データの登録が可能なカードを予め登録し、登録先のカードが予め登録されたカードかを確認すると共に正当なカードであるかを確認することにより、不正なカード、対応していないカードへの承認データの登録を防止することができる。

【0064】

【発明の効果】以上詳述したようにこの発明によれば、信用照会にかかるコストを最小限にして、しかもセキュリティを向上させることのできるカード取引システム及びカード取引方法を提供することができる。

【図面の簡単な説明】

【図1】この発明に係るカード取引システムの概略構成を示すブロック図。

【図2】各処理におけるデータのの流れの概要を示す図。

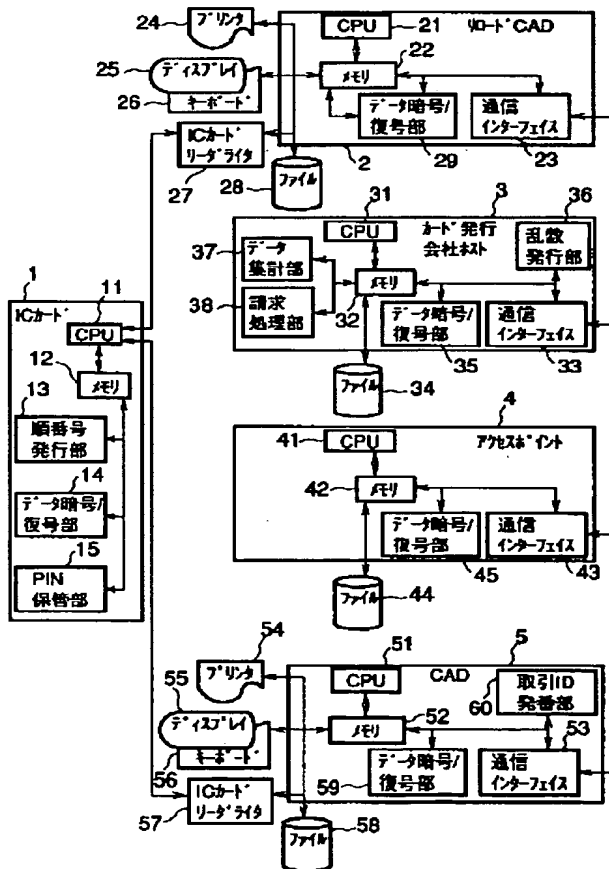
【図3】補填カードへの与信の補填処理のタイミングチャート。

【図4】補填カードへの与信の補填処理のタイミングチャート。

【図5】補填カードによる店舗での取引処理のタイミングチャート。

【図6】カード発行会社ホストへのデータ送信処理のタイミングチャート。

【図1】



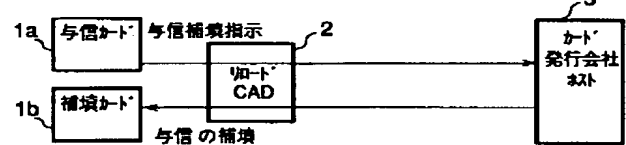
【図7】各装置の処理に必要な保持データの例を示す図。

【符号の説明】

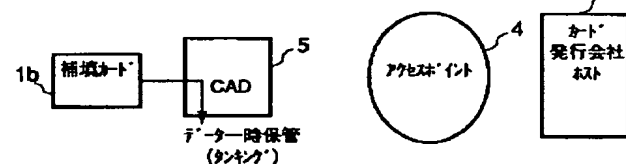
- 1…ICカード
- 1a…与信カード
- 1b…補填カード
- 2…リロードCAD
- 3…カード発行会社ホスト
- 4…アクセスポイント
- 5…CAD (Card Acceptance Device)
- 11、21、31、41、51…CPU
- 12…メモリ
- 13…順番号発行部
- 14…データ暗号/復号部
- 15…PIN保管部
- 27、57…ICカードリーダ/ライタ

【図2】

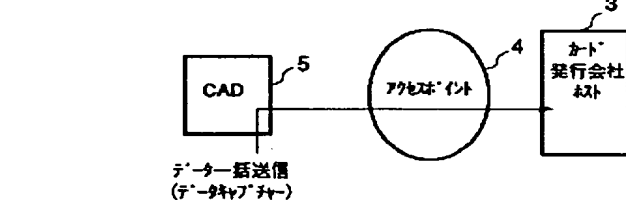
(a) ステップ1: 補填カード1bへの与信の補填



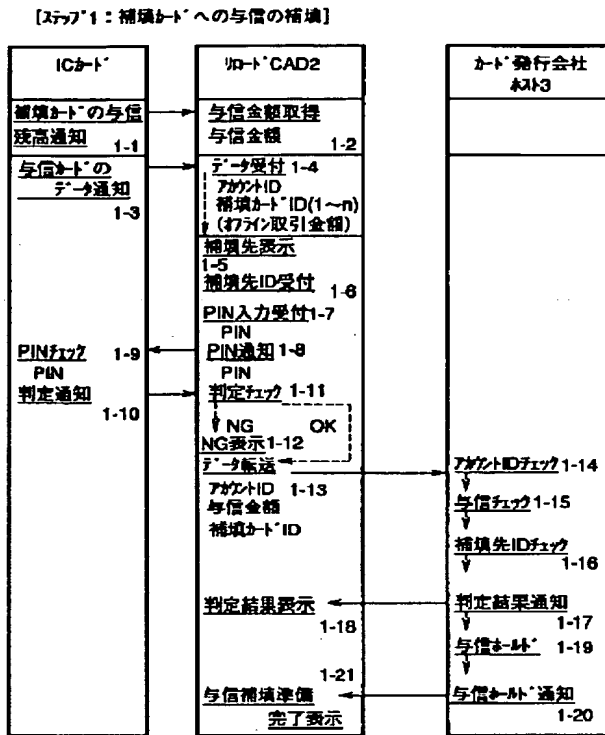
(b) ステップ2: 補填カード1bによる店舗での取引



(c) ステップ3: カード発行会社へのデータ送信



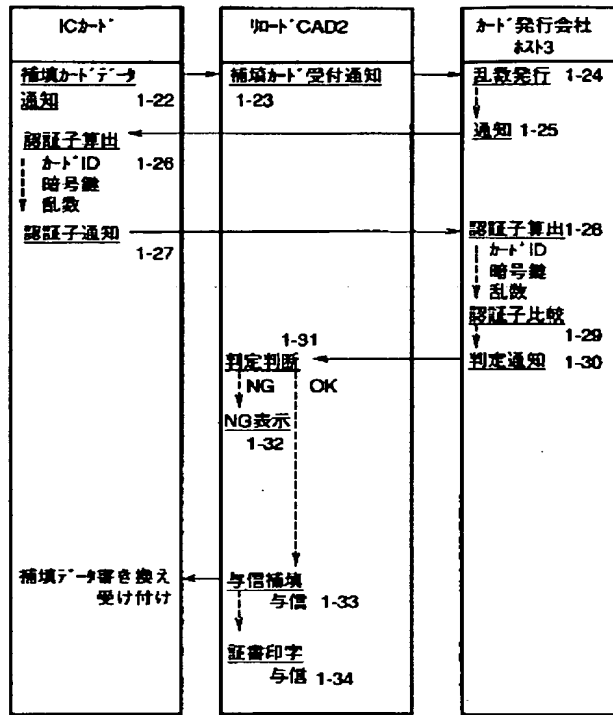
【図3】



【図5】

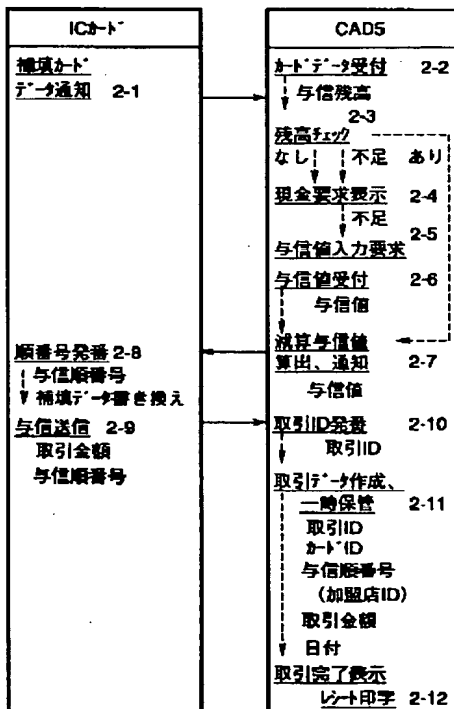
【図4】

【ステップ1：補填カードへの与信の補填(続き)】

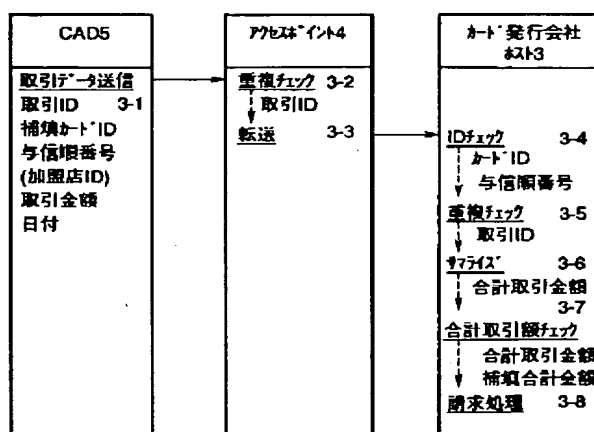


【図6】

【ステップ2：補填カードによる店舗での取引】



【ステップ3：カード発行会社へのデータ送信】



【図7】

ICカード (与信カード1a)	アカウントID 補填カードID(1～n) 与信可能限度額 カードの有効期限 与信付与方式 PIN 暗号/復号鍵
ICカード (補填カード1b)	補填カードID 与信残高 与信受け取り限度額 与信の有効期限 カードの有効期限 発番済み与信順番号 暗号/復号鍵
カードCAD2	端末ID 暗号/復号鍵
CAD5	端末ID 発番済み取引ID 暗号/復号鍵
アクセス点4	受付済み取引ID 暗号/復号鍵
カード発行会社 サイト3	与信カードに対する補填カードID(1～複数) 与信カード保持者の与信利用限度額 補填済み与信高、有効期限 使用した補填与信高 暗号/復号鍵 乱数発行用パスワード

MENU

SEARCH

INDEX

1/1



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 10063722

(43)Date of publication of application: 06.03.1998

(51)Int.Cl.

G06F 17/60
G07D 9/00
G07F 7/08

(21)Application number: 08214747

(71)Applicant:

TOSHIBA CORP

(22)Date of filing: 14.08.1996

(72)Inventor:

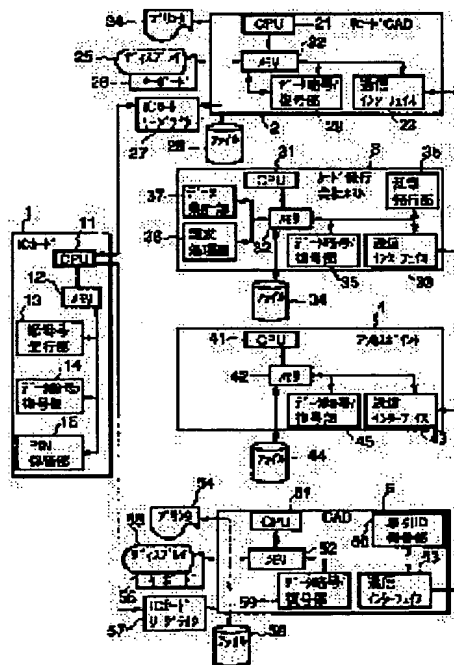
HIROKAWA KATSUHIKA
MOTAI SHOZO
TANAKA YOKO

(54) CARD TRANSACTION SYSTEM AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To minimize the cost of credit inquiry and to improve the security.

SOLUTION: A reload CAD(card acceptance device) 2 receives credit supplying instruction from an IC card 1 inserted into an IC card reader/writer 27, communicates with a card issuing company host 3, and after receiving approval (credit inquiry) from the host 3, a credit is supplied to the IC card 1. In the case of executing a transaction by a CAD 5 arranged in a store, a credit is received from the IC card 1 without executing credit inquiry to the host 3 through communication, transaction data are transmitted to an access point 4 within prescribed time, the access point 4 receives data from many CADs 5, distributes these data to the prescribed host 3 and the host 3 receives the transaction data and executes invoicing processing.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998 Japanese Patent Office

[MENU](#)

[SEARCH](#)

[INDEX](#)

HEI 10-63722

[CLAIMS]

[Claim 1]

Credit card dealing method for conducting the dealing with a credit card issued from a card issuing company, characterized in that the right for use of the predetermined amount of money approved is covered to the credit card when the right for use of said amount of money by use of said card is approved through credit inquiry to said card issuing company and said covered credit card may be used for dealing in the predetermined amount of money without credit inquiry to said card issuing company.

[Claim 2]

Credit card dealing system comprising a host computer of a card issuing company, a credit card issued from said card issuing company and a covering apparatus for covering the right for use of the predetermined amount of money to said card, characterized in that:

said host computer of card issuing company has an approving means for approving, without credit inquiry, the right for use of the predetermined amount of money for said card through the credit inquiry for said card;

said covering apparatus has a covering means for covering the right for use of the predetermined amount of money to said card when the right for use without credit inquiry of the predetermined amount of money to said card is approved by said approving means; and

said credit card has a storing means for storing the information about the right for use without credit inquiry of the predetermined amount of money covered by said covering means.

[Claim 3]

Credit card dealing method for conducting the dealing with a first credit card issued from a card issuing company, characterized in that when the right for use of the predetermined amount of money through credit inquiry to said first credit card is approved by said card issuing company, the right for use of the predetermined amount of money approved is covered to a second card corresponding to an identifier previously registered in said first card and the dealing in the predetermined amount of money covered to said second card can be performed without credit inquiry to said card issuing company.

[Claim 4]

Credit card dealing system comprising a first card issued from a card issuing company, a host computer of said card issuing company and a card covering apparatus connected to said host computer, characterized in that:

said host computer of the card issuing company has an approving means for approving the right for use without credit inquiry of the predetermined amount of money for said first card through credit inquiry of said first card; and

said card covering apparatus has a covering means for covering the right for use of the predetermined amount of money to the second card corresponding to the identifier previously registered to said first card when the right for use without credit inquiry of the predetermined amount of money for said first card is approved by said approving means.

[Claim 5]

Credit card dealing system comprising a card issued from a card issuing company, a host computer of said card issuing company and a card covering apparatus connected to said host computer, characterized in that said card has an approval instructing means for instructing getting approval of the right for use without credit inquiry of the predetermined amount of money through credit inquiry to said host computer, a storing means for storing the information about the right for use without credit inquiry of the predetermined amount of money covered by said card covering apparatus when said right for use is approved by said host computer depending on said approval instructing means and a predetermined amount of remaining money control means for allowing the dealing in the predetermined amount of money stored in said storing means without credit inquiry to said host computer of credit card issuing company.

[Claim 6]

Credit card dealing system comprising a card issued

from a card issuing company, a host computer of said card issuing company and a card covering apparatus connected to said host computer, characterized in that:

said host computer of card issuing company has a random number issuing means for issuing random numbers and a first notifying means for notifying information about random numbers issued by said random number issuing means to said card;

said card has a first receiving means for receiving random number information notified from said first notifying means, a first calculating means for calculating an authenticator based on the random number received by said first receiving means and a second notifying means for notifying the authenticator calculated by said first calculating means to said host computer of card issuing company; and

said host computer of card issuing company has a second receiving means for receiving the authenticator notified from said second notifying means, a second calculating means for calculating an authenticator based on the random number issued by said random number issuing means, a comparing means for comparing the authenticator calculated by said second calculating means with the authenticator received by said second receiving means and an approving means for approving the justice of said card when comparison results of said comparing means are matched.

[Claim 7]

Credit card certifying method characterized in certifying that a card is proved as a justified card based on the comparison result through the processes that said host computer of card issuing company issues random numbers which cannot be assumed by said card issued from the card issuing company and then notifies said random numbers to said card, said card calculates the authenticator based on such random numbers and then notifies said authenticator to said host computer and said host computer also calculates the authenticator based on said random numbers and compares said calculated authenticator with the authenticator notified from said card.

[0013]

[Preferred Embodiment]

A preferred embodiment of the present invention will be explained with reference to the accompanying drawings. Fig. 1 schematically illustrates a structure of the card dealing system of the present invention. Namely, the card dealing system is composed of an IC card 1 issued from a card issuing company, a reloading CAD (Card Acceptance Device) 2 for covering credit assurance, a host computer of card issuing company, an access point 4 and a CAD 5 provided in the shop for dealing.

[0014]

An IC card 1 may be classified, although not illustrated, into a credit assuring card 1a having a credit function for instructing the covering of credit assurance and a covering card 1b which can realize the dealing based on the credit assurance by covering credit assurance. Moreover, the IC card 1c integrating the credit assuring card and covering card may also be used.

[0015]

Since the IC cards 1, 1a, 2b, 1c have the identical structure, the structure of the IC card 1 illustrated will be explained. Namely, the IC card 1 is composed of a CPU11, a memory 12, a sequential number generating means 13, a data ciphering/deciphering means 14 and a PIN storing means 15.

[0016]

The CPU11 performs transmission/reception of data and commands to/from the IC card reader/writer 27 or 57 and check of PIN (Personal Identification Number) existing in the PIN storing means 15. In the memory 12 as the storing means, data required for processes is stored. The sequential number issuing means 13 issues unique sequential numbers for credit assurance to be paid when the dealing is performed using the covered credit assurance. The sequential numbers issued are paid together with credit assurance to a dealing partner for the purpose of checking doubled credit assurance.

[0017]

The data ciphering/deciphering means 14 ciphers the data to be sent to the reload CAD2 or CAD5 and decipheres the ciphered data from the reload CAD2 or CAD5 and also calculates the authenticator based on the random numbers notified from the card issuing company host computer 3.

[0018]

The CAD2 is a CAD for receiving the instruction for covering of credit assurance, making communication with the card issuing company host computer 3 and covering credit assurance to the predetermined IC card 1 after approval by the card issuing company host computer 3, being composed of a CPU21, a memory 22, a communication interface 23, a printer 24, a display 25, a keyboard 26, an IC card reader/writer 27, a file 28 and a data ciphering/deciphering means 29.

[0019]

The CPU21 controls each device to issue the instructions for exchange of data with IC card 1, data check and data writing to the IC card 1 or the like. Various pieces of information are recorded to the memory 22. The communication interface 23 exchanges data with the card issuing company host computer 3 to develop such data to the memory 22.

[0020]

The printer 24 issues a certificate when the covering is completed. The display 25 displays the message or data required for credit assurance covering process. The

keyboard 26 accepts PIN for instructing the covering of credit assurance and an input of covering destination and then transfers such data to the memory 22. The IC card reader/writer 27 writes or reads data to or from the IC card 1.

[0021]

A file 28 stores the softwares and data required for the covering process. The data ciphering/deciphering means 29 ciphers the data to be sent to the IC card 1 or the card issuing company host computer 3 and deciphers a part of the ciphered data from the IC card 1 or the card issuing company host computer 3.

[0022]

The card issuing company host computer 3 approves the dealing based on the credit assurance condition of an owner of the issued IC card 1 (card holder), accepts the dealing data and then issues a bill later to the owner of each IC card 1 (card holder). A card holder makes payment for the amount of dealing to each shop. The card issuing company host computer 3 is composed of a CPU31, a memory 32, a communication interface 33, a file 34, a data ciphering/deciphering means 35, a random number issuing means 36, a data collecting means 37 and a bill issuing means 38.

[0023]

The CPU31 controls each device. Various pieces of data are recorded to the memory 32. The communication

interface 33 performs data exchange with reload CAD2 and access point 4 to develop such data to the memory 32. The file 34 stores the softwares and data required for covering of credit assurance, collection of dealing data and issuance of bill.

[0024]

The data ciphering/deciphering means 35 ciphers the data to be sent to the reload CAD2 or access point 4 and deciphers the ciphered data from the reload CAD2 or access point 4 and also calculates the authenticator based on the random numbers issued by the random number issuing means 36. The random number issuing means 36 issues the random numbers to prove whether the IC card 1 can be qualified or not for the covering of credit assurance. This random number is notified to the IC card 1 and the IC card 1 calculates the authenticator based on this random number and then notifies the result to the card issuing company host computer 3.

[0025]

The data collecting means 37 collects the dealing data transmitted from the access point 4 for each IC card 1. The collected data is used to check whether the value of credit assurance used for dealing has exceeded or not the previously covered credit assurance. The bill issuing means 38 issues a bill to the owner of the IC card 1 (card holder) based on the dealing data.

[0026]

The access point 4 accepts the data of many CAD5 and then shares such data to the predetermined card issuing company host computer 3. The access point 4 is composed of a CPU4, a memory 42, a communication interface 43, a file 44 and a data ciphering/deciphering means 45. The CPU41 controls each device. The memory 42 records various pieces of data. The communication interface 43 performs data exchange with the card issuing company host computer 3 and CAD5 to develop the data to the memory 42. The file 4 stores the softwares and data required for sharing the data. The date ciphering/deciphering means 45 decipheres a part of the ciphered data to be sent to the card issuing company host computer 3 from CAD5 or to CAD5 from the card issuing company host computer 3.

[0027]

CAD5 is a CAD for accepting credit assurance from the IC card 1 at the time of dealing and transmits the dealing data to the access point 4 at the predetermined time and is composed of a CPU51, a memory 52, a communication interface 53, a printer 54, a display 55, a keyboard 56, an IC card reader/writer 57, a file 58, a data ciphering/deciphering means 59 and a dealing ID number issuing means 60.

[0028]

The CPU51 controls each device to issue the instruction for data exchange with IC card 1, data check and data writing to IC card 1 or the like. The memory

52 stores various pieces of data. The communication interface 53 performs data exchange with the card issuing company host computer 3 to develop the data to the memory 52. The printer 54 issues a certificate when the dealing is completed.

[0029]

The display 55 displays the messages or data required for dealing process. The keyboard 56 accepts an input of credit assurance value if credit assurance is short and then transfers such data to the memory 52. The IC card reader/writer 57 reads or writes data from or to the IC card 1. The file 58 stores softwares and data required for dealing process.

[0030]

The data ciphering/deciphering means 59 ciphers data to be sent to the IC card 1 or card issuing company host computer 3 and deciphers a part of the ciphered data from the IC card 1 or card issuing company host computer 3. The dealing ID number issuing means 60 issues the numbering of dealing ID at the time of generating the dealing data. The dealing ID is given uniquely to each dealing data to be used for checking double-issuing of dealing data.

Fig. 1:

15: PIN storing means; 27: IC card reader/writer;

57: IC card reader/writer;

【図1】 Figure 1

